

mrf



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/579,035	05/26/2000	Sadeg M. Faris	105-081USANDO	8056
26665	7590	08/15/2006	EXAMINER	
REVEO, INC. 3 WESTCHESTER PLAZA ELMSFORD, NY 10523			BORISSOV, IGOR N	
			ART UNIT	PAPER NUMBER
			3639	
DATE MAILED: 08/15/2006				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/579,035	Applicant(s) FARIS ET AL.	
	Examiner Igor Borissov	Art Unit 3639	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 June 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 374-379 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 374-379 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

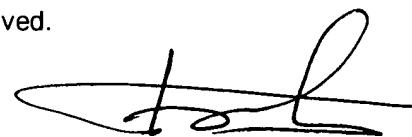
Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.



IGOR N. BORISSOV
PRIMARY EXAMINER

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Amendment received on 6/07/2006 is acknowledged and entered. Claims 1-373 have previously been canceled. Claims 374 and 376-379 have been amended. Claims 374-379 are currently pending in the application.

Specification

The disclosure is objected to because of the following informalities:

Lines 34 and last line on each page appear to be illegible and have missing words.

Appropriate corrections are required.

Claim Objections

Claims Objections have been withdrawn due to applicant's amendment.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 376 and 378 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 376 include the following phrase in parentheses: "(or WWW server connected thereto)". The use of parentheses is confusing, because it is not clear should the limitation in the parentheses be given patentable weight, or not.

Claim 378 includes the following phrase in preamble: "(sub)network". The use of parentheses is confusing, because it is not clear should the limitation in the parentheses be given patentable weight or not.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 374, 375, 377 and 379 are rejected under 35 U.S.C. 103(a) as being unpatentable over Murphy (US 6,317,500) in view of Alcorn et al. (US 6,104,815) and further in view of Teare et al. (US 5,243,652).

Claims 374 and 379. Murphy teaches a method and system for location-sensitive decryption of an encrypted signal, comprising:

downloading encrypted content over a network to a remote network computing device (receiver) (C. 7, L. 30-55);

embodying a global positioning system (GPS) chip into said network computing device (C. 6, L. 46-56);

programming said GPS chip in said network computing device so as to decrypt said encrypted content only when said computing device is present in an authorized (licensed) site location (C. 6, L. 46-56);

disposing said network computing device at said authorized location so as to automatically enable said network computing device to decrypt said encrypted content (C. 6, L. 46-56),

wherein said content is visually or sonically presented by the device (C. 7, L. 36-37).

While generating time coordinates is obvious feature of GPS technology, Murphy does not explicitly teach said feature. Also, Murphy does not specifically teach that said network is the Internet. Also, Murphy does not specifically teach that said device decrypts said encrypted content at a time different from said downloading.

Alcorn et al. (Alcorn) teaches a method and system for providing encrypted communication between a remote network computing device (receiver) and a server, said remote network computing device including a GPS unit for generating geographical and time coordinates, and an encryption/decryption unit for enabling secure communication with said server over the Internet (C. 5, L. 16-21; C. 6, L. 28-33, 39-40, 54-56), wherein said server authorizes said network computing device to access a content only if said network computing device is in a valid location and at the valid time (C. 7, L. 14-17, 23-25).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Murphy to include generating time coordinates and transmitting said time coordinates together with geographical coordinates to a secure server, as disclosed in Alcorn, because it would advantageously allow to enhance the security of the system thereby preventing possible fraudulent activity with the receiver. And It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Murphy and Alcorn to include that said communication is conducted over the Internet, as disclosed in Alcorn, because it would advantageously allow to save funds by using the existing largest network rather than investing into a dedicated one.

Teare et al. (Teare) teaches a method for accessing location-sensitive data, wherein a mobile device having encrypted programmed material onboard travels in space and time, and wherein, upon detecting that time-position signature data of said device matches a predetermined value, said device is enabled to decrypt its encrypted programmed material (C. 1, L. 40-55; C. 2, L. 1-6).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Murphy and Alcorn to include that said device decrypts said encrypted content at a time different from said downloading, as disclosed in Teare, because it would advantageously allow to provide location-sensitive control over a mobile system in a secure manner, as specifically stated in Teare (C. 1, L. 32-37).

Claim 375. Alcorn teaches transmitting by said receiver a digitally-signed data package to a time and space (TS)-stamping tracking server for receiving and processing said digitally-signed data indicative that said network computing device is present at said predetermined TS coordinates and automatically transmitting said package back to said receiver to enable said receiver to access said content (C. 3, L. 60-62; C. 10, L. 18-22, 56-61). The motivation to combine the references would be to enhance the security of the system thereby preventing possible fraudulent activity with the receiver.

Claim 377. Murphy teaches said method and system for location-sensitive decryption of an encrypted signal, comprising:

- downloading encrypted content over a network to a remote network computing device (receiver) (C. 7, L. 30-55);

- embodying a global positioning system (GPS) chip into said network computing device (C. 6, L. 46-56);

- programming said GPS chip in said network computing device so as to decrypt said encrypted content only when said computing device is present in an authorized (licensed) site location (C. 6, L. 46-56);

- disposing said network computing device at said authorized location so as to automatically enable said network computing device to decrypt said encrypted content (C. 6, L. 46-56),

- wherein said content is visually or sonically presented by the device (C. 7, L. 36-37); and

- disposing said network computing device at said authorized location so that said network computing device is enabled to access a prescribed communication network (C. 7, L. 30-55).

While generating time coordinates is obvious feature of GPS technology, Murphy does not explicitly teach said feature. Also, Murphy does not specifically teach that:

- said network is the Internet; and

said "enabling" of said network computing device includes enabling said network computing device by a TS-stamping tracking server.

Also, Murphy does not specifically teach that said device decrypts said encrypted content at a time different from said downloading.

Alcorn teaches said method and system for providing encrypted communication between a remote network computing device (receiver) and a server, said remote network computing device including a GPS unit for generating geographical and time coordinates, and an encryption/decryption unit for enabling secure communication with a TS-stamping tracking server over the Internet (C. 5, L. 16-21; C. 6, L. 28-33, 39-40; 54-56), wherein said TS-stamping tracking server authorizes (enables) said network computing device to access a content only if said network computing device is in a valid location and at the valid time (C. 7, L. 14-17, 23-25).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Murphy to include generating time coordinates and transmitting said time coordinates together with geographical coordinates to said TS-stamping tracking server for enabling said network computing device, as disclosed in Alcorn, because it would advantageously allow to enhance the security of the system thereby preventing possible fraudulent activity with the receiver. And It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Murphy and Alcorn to include that said communication is conducted over the Internet, as disclosed in Alcorn, because it would advantageously allow to save funds by using the existing largest network rather than investing into a dedicated one.

Teare et al. (Teare) teaches a method for accessing location-sensitive data, wherein a mobile device having encrypted programmed material onboard travels in space and time, and wherein, upon detecting that time-position signature data of said device matches a predetermined value, said device is enabled to decrypt its encrypted programmed material (C. 1, L. 40-55; C. 2, L. 1-6).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Murphy and Alcorn to include that said device decrypts said encrypted content at a time different from said downloading, as disclosed in Teare,

Art Unit: 3639

because it would advantageously allow to provide location-sensitive control over a mobile system in a secure manner, as specifically stated in Teare (C. 1, L. 32-37).

Claims 376 and 378 are rejected under 35 U.S.C. 103(a) as being unpatentable over Murphy in view of Alcorn et al. and further in view of Dowling et al. (US 6,522,875).

Claim 376. Murphy teaches said method and system for location-sensitive decryption of an encrypted signal, comprising:

- downloading encrypted content over a network to a remote network computing device (receiver) (C. 7, L. 30-55);

- embodying a global positioning system (GPS) chip into said network computing device (C. 6, L. 46-56);

- programming said GPS chip in said network computing device so as to decrypt said encrypted content only when said computing device is present in an authorized (licensed) site location (C. 6, L. 46-56);

- disposing said network computing device at said authorized location so as to automatically enable said network computing device to decrypt said encrypted content (C. 6, L. 46-56),

- wherein said content is visually or sonically presented by the device (C. 7, L. 36-37);

- tracking the exact location of said network computing device (C. 8, L. 9-18);

- notifying authorities (an enforcement agency) that unauthorized action is performed with said GPS-enabled computing device (C. 8, L. 19-28).

While generating time coordinates is obvious feature of GPS technology, Murphy does not explicitly teach said feature. Also, Murphy does not specifically teach that:

- said network is the Internet;

- said tracking the exact location of said network computing device is performed by a TS-stamping tracking server; and

Art Unit: 3639

said enabling of said network computing device includes partially enabling said network computing device while being outside of the authorized location.

Also, Murphy does not specifically teach that said device decrypts said encrypted content at a time different from said downloading.

Alcorn teaches said method and system for providing encrypted communication between a remote network computing device (receiver) and a server, said remote network computing device including a GPS unit for generating geographical and time coordinates, and an encryption/decryption unit for enabling secure communication with a TS-stamping tracking server over the Internet (C. 5, L. 16-21; C. 6, L. 28-33, 39-40, 54-56), wherein said TS-stamping tracking server authorizes said network computing device to access a content only if said network computing device is in a valid location at the valid time (tracking feature) (C. 7, L. 14-17, 23-25).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Murphy to include generating time coordinates and transmitting said time coordinates together with geographical coordinates to a secure server, as disclosed in Alcorn, because it would advantageously allow to enhance the security of the system thereby preventing possible fraudulent activity with the receiver. And it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Murphy and Alcorn to include that said communication is conducted over the Internet, as disclosed in Alcorn, because it would advantageously allow to save funds by using the existing largest network rather than investing into a dedicated one.

Dowling et al. (Dowling) teaches a method and system for geographical web browser, comprising a mobile network computing device (a mobile unit) equipped with a GPS unit and a browser, and a communication server, wherein said communication server controls flow of information to said mobile unit based on GPS (location) information received, thereby suggesting partial enabling of said mobile unit (C. 3, L. 1-3; C. 4, L. 31-42).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Murphy and Alcorn to include that said enabling of said

Art Unit: 3639

network computing device includes partially enabling said network computing device while being outside of the authorized location as suggested in Dowling, because it would advantageously allow to limit information provided to a user of said network computing device to information which is specific to a particular geographic location, thereby decreasing time required for processing said information limited an amount of information.

Teare et al. (Teare) teaches a method for accessing location-sensitive data, wherein a mobile device having encrypted programmed material onboard travels in space and time, and wherein, upon detecting that time-position signature data of said device matches a predetermined value, said device is enabled to decrypt its encrypted programmed material (C. 1, L. 40-55; C. 2, L. 1-6).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Murphy, Alcorn and Dowling to include that said device decrypts said encrypted content at a time different from said downloading, as disclosed in Teare, because it would advantageously allow to provide location-sensitive control over a mobile system in a secure manner, as specifically stated in Teare (C. 1, L. 32-37).

Claim 378. Murphy teaches said method and system for location-sensitive decryption of an encrypted signal, comprising:

downloading encrypted content over a network to a remote network computing device (receiver) (C. 7, L. 30-55);

programming said GPS chip in said network computing device so as to decrypt said encrypted content only when said computing device is present in an authorized (licensed) site location (C. 6, L. 46-56);

wherein said content is visually or sonically presented by the device (C. 7, L. 36-37);

tracking the exact location of said network computing device (C. 8, L. 9-18);

notifying authorities (an enforcement agency) that unauthorized action is performed with said GPS-enabled computing device (C. 8, L. 19-28).

Art Unit: 3639

Murphy does not specifically teach that:

said tracking the exact location of said network computing device is performed by a TS-stamping tracking server;

said network is the Internet; and

said enabling of said network computing device includes partially enabling said network computing device while being outside of the authorized location.

Also, Murphy does not specifically teach that said device decrypts said encrypted content at a time different from said downloading.

Alcorn teaches said method and system for providing encrypted communication between a remote network computing device (receiver) and a server, said remote network computing device including an encryption/decryption unit for enabling secure communication with a TS-stamping tracking server over the Internet (C. 5, L. 16-21; C. 6, L. 28-33, 39-40, 54-56), wherein said TS-stamping tracking server authorizes said network computing device to access a content only if said network computing device is in a valid location at the valid time (tracking feature) (C. 7, L. 14-17, 23-25).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Murphy to include that said tracking the exact location of said network computing device is performed by a TS-stamping tracking server, as disclosed in Alcorn, because it would advantageously allow to enhance the security of the system thereby preventing possible fraudulent activity with the receiver. And it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Murphy and Alcorn to include that said communication is conducted over the Internet, as disclosed in Alcorn, because it would advantageously allow to save funds by using the existing largest network rather than investing into a dedicated one.

Dowling teaches a method and system for geographical web browser, comprising a mobile network computing device (a mobile unit) equipped with a GPS unit and a browser, and a communication server, wherein said communication server controls flow of information to said mobile unit based on GPS (location) information received, thereby suggesting partial enabling of said mobile unit (C. 3, L. 1-3; C. 4, L. 31-42).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Murphy and Alcorn to include that said enabling of said network computing device includes partially enabling said network computing device while being outside of the authorized location as suggested in Dowling, because it would advantageously allow to limit information provided to a user of said network computing device to information which is specific to a particular geographic location, thereby decreasing time required for processing said information limited an amount of information.

Teare et al. (Teare) teaches a method for accessing location-sensitive data, wherein a mobile device having encrypted programmed material onboard travels in space and time, and wherein, upon detecting that time-position signature data of said device matches a predetermined value, said device is enabled to decrypt its encrypted programmed material (C. 1, L. 40-55; C. 2, L. 1-6).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Murphy, Alcorn and Dowling to include that said device decrypts said encrypted content at a time different from said downloading, as disclosed in Teare, because it would advantageously allow to provide location-sensitive control over a mobile system in a secure manner, as specifically stated in Teare (C. 1, L. 32-37).

Response to Arguments

Applicant's arguments filed 6/07/2006 have been fully considered but they are not persuasive.

In response to applicant's argument that the prior art fails to disclose that said mobile device decrypts said encrypted content at a time different from the time of downloading of said content, it is noted that Teare explicitly teaches said feature. Specifically, Teare teaches a mobile device having encrypted programmed material onboard which travels in space and time, and wherein, upon detecting that time-position

signature data of said device matches a predetermined value, said device is enabled to decrypt its encrypted programmed material (C. 1, L. 40-55; C.2, L. 1-6).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Igor Borissov whose telephone number is 571-272-6801. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John W. Hayes can be reached on 571-272-6708. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 3639

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

IB
8/09/2006